



CHAPTER 42

Monitoring Properties

Properties contains the following topics:

- [AAA Servers](#)
- [CRL](#)
- [Connection Graphs](#)
- [DNS Cache](#)
- [Device Access](#)
- [IP Audit](#)
- [System Resources Graphs](#)

AAA Servers

The AAA Server pane lets you view the AAA Server configuration.

Prerequisites

None.

Fields

The AAA Server pane displays the following fields:

- **Server Group**—Displays a configured server group, or LOCAL if none have been configured.
- **Protocol**—Displays what protocol the server group uses for AAA.
- **IP Address**—Displays the IP address of the configured AAA server.

Below the list of AAA servers are the statistics for each configured server. You can clear the statistics using the Clear Server Stats button.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CRL

This pane allows you to view or clear associated CRLs of selected Trustpoints. Trustpoints are configured in Configuration > Device Administration > Certificates > Trustpoints.

Fields

- Trustpoint name—The name of the selected Trustpoint.
- View CRL—View the selected CRL.
- Clear CRL—Clear the selected CRL from the cache.
- CRL info—*Display only*. Displays detailed CRL information.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Connection Graphs

The Connection Graphs pane let you view connection information about the security appliance in graph format. You can view information about NAT and performance monitoring information, including UDP connections, AAA performance, and inspection information. Refer to the following topics for more information:

- [Xlates](#)
- [Perfmom](#)

Xlates

Xlates lets you view the active Network Address Translations in a graph format. You can graph a maximum of four graphs in one frame.

Fields

- Available Graphs For:—Lists the components you can graph.

- Xlate Utilization—Displays the security appliance NAT utilization.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- Add—Click this button to move the selected entries in the Available Graphs For field to the Selected Graphs field.
- Remove—Removes the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Perfmon

The Perfmon pane lets you view the performance information in a graph format. You can graph a maximum of four graphs in one frame.

This information includes the number of translations, connections, Websense requests, address translations, and AAA transactions that occur each second.

Fields

- Available Graphs For:—Lists the components you can graph.
 - AAA Perfmon—Displays the security appliance AAA performance information.
 - Inspection Perfmon—Displays the security appliance inspection performance information.
 - Web Perfmon—Displays the security appliance web performance information, including URL access and URL server requests.
 - Connections Perfmon—Displays the security appliance connections performance information.
 - Xlate Perfmon—Displays the security appliance NAT performance information.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- Add—Click this button to move the selected entries in the Available Graphs For field to the Selected Graphs field.
- Remove—Removes the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

DNS Cache

The security appliance provides a local cache of DNS information from external DNS queries sent out for certain WebVPN and Certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache along with its corresponding hostname.

Important Notes

- DNS cache entries are time stamped. The time stamp will be used to age out unused entries. When the entry is added to the cache the time stamp is initialized. Each time the entry is accessed the timestamp is updated. At a configured time interval, the DNS cache will check all entries and purge those entries whose time exceeds a configured age out timer.
- If new entries arrive but there is no room in the cache, since the size exceeded or there is no more memory allowed, the cache will be thinned by one third based on entries age. The oldest entries will be removed.
- The entire cache can be cleared by clicking the **Clear Cache** button.

Fields

- Host—The DNS name of the host.
- IP Address—Shows the address that resolves to the hostname.
- Permanent—Indicates if the entry made though a **name** command.
- Idle Time—Gives the time elapsed since the security appliance last referred to that entry.
- Active—Indicates if the entry has aged out. If there is no sufficient space in cache, this entry may be deleted.
- Clear Cache—Clears the DNS cache.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Device Access

Device Access lets you monitor management sessions, AAA locked out users, and authenticated users.

Device Access contains the following topics:

- [AAA Local Locked Out Users](#)
- [Authenticated Users](#)
- [HTTPS/ASDM Sessions](#)
- [Secure Shell Sessions](#)
- [Telnet Sessions](#)

AAA Local Locked Out Users

The AAA Local Locked Out Users pane lets you view a list of users who have been locked out of ASDM for failed login attempts. You can also clear selected lockout conditions or all lockouts.

Fields

The AAA Local Lockouts area displays the following.

- Currently locked out users—A list of the currently locked out users.
- Lock Time—The amount of time the user has been locked out from accessing the system.
- Failed Attempts—The number of failed login attempts.
- User—The user name used with the failed login attempts.

The following buttons are also available:

- Refresh—Updates the display with the most current information.
- Clear lockout—Clears the selected user lockout condition.
- Clear all lockouts—Clears all user lockout conditions. It is good practice to refresh the list of lockout conditions before clearing all lockouts.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Authenticated Users

This pane lets you view what users are authenticated to the security appliance.

Fields

- User—Displays the user name of the person authenticated to the security appliance.

- IP Address—Displays the IP address of the user authenticated to the security appliance.
- Dynamic ACL—Displays the dynamic access list of the user authenticated to the security appliance.
- Inactivity Timeout—Displays the amount of time the selected user must remain inactive before the session times out and the user is disconnected.
- Absolute Timeout—Displays the amount of time the selected user can remain connected before the session closes and the user is disconnected.
- Refresh—Select to refresh the list of currently authenticated users.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

HTTPS/ASDM Sessions

The HTTPS/ASDM pane lets you view currently connected HTTPS/ASDM sessions.

A secure connection is needed so that a PC or workstation client running ASDM in a network browser window can communicate with the security appliance.

Fields

The HTTPS/ASDM pane displays the following fields:

- Session ID—Displays the name of a connected HTTPS/ASDM session.
- IP Address—Displays the IP address of each host or network permitted to connect to this security appliance.
- Refresh—Select to refresh the list of currently connected HTTPS/ASDM sessions.
- Disconnect—Select to disconnect a connected HTTPS/ASDM session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Secure Shell Sessions

The Secure Shell Sessions pane lets you view hosts connected to the security appliance for administrative access using the SSH protocol.

Fields

The Currently Connected Secure Shell Sessions pane displays the following fields:

- Client—Displays the client type for the selected SSH session.
- User—Displays the user name for the selected SSH session.
- State—Displays the state of the selected SSH session.
- Version—Displays the version of SSH used to connect to the security appliance.
- Encryption (in)—Displays the inbound encryption method used for the selected session.
- Encryption (out)—Displays the outbound encryption method used for the selected session.
- HMAC (in)—Displays the configured HMAC for the selected inbound SSH session.
- HMAC (out)—Displays the configured HMAC for the selected outbound SSH session.
- SID—Displays the secure ID of the selected session.
- Refresh—Select to refresh the list of currently connected SSH sessions.
- Disconnect—Select to disconnect a connected SSH session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Telnet Sessions

The Telnet Sessions pane lets you view currently connected Telnet sessions.

Fields

The Telnet Sessions pane displays the following fields:

- Session ID—Displays the name of a connected Telnet sessions.
- IP Address—Displays the IP address of each host permitted to connect to this security appliance over Telnet.
- Refresh—Select to refresh the list of currently connected Telnet sessions.
- Disconnect—Select to disconnect a connected Telnet session.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

IP Audit

The IP Audit pane lets you view the number of packets that match informational and attack signatures in graph or table form. Each statistic type shows the combined packets for all interfaces that have IP audit enabled.

Fields

- Available Graphs for—Lists the types of signatures available for monitoring. See [IP Audit Signatures](#) for detailed information about each signature type. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.
 - IP Options—Shows the packet count for the following signatures:
 - Bad Options List (1000)
 - Timestamp (1002)
 - Provide s, c, h, tcc (1003)
 - SATNET ID (1005)
 - IP Route Options—Shows the packet count for the following signatures:
 - Loose Source Route (1004)
 - Record Packet Route (1001)
 - Strict Source Route (1006)
 - IP Attacks—Shows the packet count for the following signatures:
 - IP Fragment Attack (1100)
 - Impossible IP Packet (1102)
 - IP Teardrop (1103)
 - ICMP Requests—Shows the packet count for the following signatures:
 - Echo Request (2004)
 - Time Request (2007)
 - Info Request (2009)
 - Address Mask Request (2011)
 - ICMP Responses—Shows the packet count for the following signatures:
 - Echo Reply (2000)
 - Source Quench (2002)
 - Redirect (2003)
 - Time Exceeded (2005)

- Parameter Problem (2006)
- ICMP Replies—Shows the packet count for the following signatures:
 - Unreachable (2001)
 - Time Reply (2008)
 - Info Reply (2010)
 - Address Mask reply (2012)
- ICMP Attacks—Shows the packet count for the following signatures:
 - Fragmented ICMP (2150)
 - Large ICMP (2151)
 - Ping of Death (2154)
- TCP Attacks—Shows the packet count for the following signatures:
 - No Flags (3040)
 - SYN & FIN Flags Only (3041)
 - FIN Flag Only (3042)
- UDP Attacks—Shows the packet count for the following signatures:
 - Bomb (4050)
 - Snork (4051)
 - Chargen (4052)
- DNS Attacks—Shows the packet count for the following signatures:
 - Host Info (6050)
 - Zone Transfer (6051)
 - Zone Transfer High Port (6052)
 - All Records (6053)
- FTP Attacks—Shows the packet count for the following signatures:
 - Improper Address (3153)
 - Improper Port (3154)
- RPC Requests to Target Hosts—Shows the packet count for the following signatures:
 - Port Registration (6100)
 - Port Unregistration (6101)
 - Dump (6102)
- YP Daemon Portmap Requests—Shows the packet count for the following signatures:
 - ypserv Portmap Request (6150)
 - yplib Portmap Request (6151)
 - yppasswdd Portmap Request (6152)
 - ypupdated Portmap Request (6153)
 - ypxfrd Portmap Request (6154)
- Miscellaneous Portmap Requests—Shows the packet count for the following signatures:
 - mountd Portmap Request (6155)

- rexd Portmap Request (6175)
 - Miscellaneous RPC Calls—Shows the packet count for the following signatures:
 - rexd Attempt (6180)
 - RPC Attacks—Shows the packet count for the following signatures:
 - statd Buffer Overflow (6190)
 - Proxied RPC (6103)
- Add—Adds the selected statistic type to the selected graph window.
- Remove—Removes the selected statistic type from the selected graph window.
- Show Graphs—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included on the graph are shown in the Selected Graphs pane, to which you can add additional types. Graph windows are named for ASDM followed by the interface IP address and the name “Graph”. Subsequent graphs are named “Graph (2)” and so on.
- Selected Graphs—Shows the statistic types you want to show in the selected graph window. You can include up to four types.
 - Show Graphs—Shows the graph window or updates the graph with additional statistic types if added.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Resources Graphs

System Resources Graphs lets you view the status of the security appliance memory, CPU, and block utilization. You can graph a maximum of four graphs in one frame.

System Resources Graphs contains the following topics:

- [Blocks](#)
- [CPU](#)
- [Memory](#)

Blocks

Blocks lets you view the free and used memory blocks in a graph format. You can graph a maximum of four graphs in one frame.

Fields

- Available Graphs For:—Lists the components you can graph.
 - Blocks Used—Displays the security appliance used memory blocks.
 - Blocks Free—Displays the security appliance free memory blocks.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- Add—Click this button to move the selected entries in the Available Graphs For field to the Selected Graphs field.
- Remove—Removes the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

CPU

CPU lets you view the CPU utilization in a graph format. You can graph a maximum of four graphs in one frame.

Fields

- Available Graphs For:—Lists the components you can graph.
 - CPU Utilization—Displays the security appliance CPU utilization.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- Add—Click this button to move the selected entries in the Available Graphs For field to the Selected Graphs field.
- Remove—Removes the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Memory

Memory lets you view the memory utilization in a graph format. You can monitor free and used memory available in real time. You can graph a maximum of four graphs in one frame.

Fields

- Available Graphs For:—Lists the components you can graph.
 - Free Memory—Displays the security appliance free memory.
 - Used Memory—Displays the security appliance used memory.
- Graph Window—Shows the graph window name to which you want to add a statistic type. If you have a graph window already open, a new graph window is listed by default. If you want to add a statistic type to an already open graph, select the open graph window name. The statistics already included in the graph window are shown in the Selected Graphs field, to which you can add additional types (up to a maximum of four types per window).
- Add—Click this button to move the selected entries in the Available Graphs For field to the Selected Graphs field.
- Remove—Removes the selected statistic type from the Selected Graphs field.
- Show Graphs—Click to display a new or updated graph window with the selected statistics.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—